

⑧ (1) 文献

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-151578

(43)Date of publication of application : 30.05.2000

(51)Int.Cl.

H04L 9/14

G07B 15/00

H04Q 7/38

(21)Application number : 10-318605

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 10.11.1998

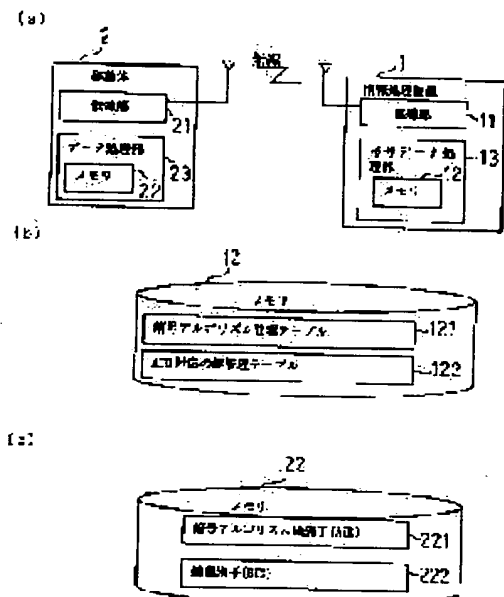
(72)Inventor : MORIYOSHI KUNIHARU
TOKITA TOSHIO

(54) ENCRYPTION COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an encryption communication system where a mobile body and an information processing unit can process encryption communication by ensuring security of an encryption test possessed by the mobile body.

SOLUTION: A mobile body has plural encryption algorithm identifier AID 221 and a key identifier KID 222 of an encryption key/decoding key corresponding to the AID and an information processing unit has a plurality of encryption algorithm sets, the encryption algorithm identifier AID 221 corresponding to each encryption algorithm, a plurality of encryption keys/decoding keys corresponding to each encryption algorithm, the key identifier KID 222 corresponding to each encryption key/decoding key.



LEGAL STATUS

[Date of request for examination]

24.12.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

[0015]

[Means of solving the problems]

The encryption communication device according to the first invention consisting of an information processing unit and a plurality of mobile bodies to mutually communicate with the information processing device, wherein each of the mobile bodies includes a means for receiving a cipher text transmitted from the information processing device, a first storing means to store a unique encryption algorithm identifier, a unique key identifier as well as the cipher text received, and a means for transmitting the encryption algorithm identifier, the key identifier and the cipher text stored in the first storing means to the information processing device, when its position from the information processing device attains a prescribed position, the information processing device includes a means for receiving the cipher text, encryption algorithm identifier and the key identifier transmitted from mobile bodies located at the prescribed position, a second storing means to store a plurality of different algorithms each corresponding to the encryption algorithm identifiers held by each of the plurality of mobile bodies, and a plurality of different keys each corresponding to the key identifiers held by each of the plurality of mobile bodies, a selecting means including a means for selecting a key corresponding to the received encryption algorithm identifier from among the plurality of algorithms stored in the second storing means, and a means for selecting an algorithm corresponding to the received encryption algorithm identifier from among the plurality of algorithms stored in the second storing means, a decrypting means for decrypting the received cipher text with the key selected by the selecting means using the algorithm selected by the selecting means, an encrypting means for generating a new cipher text with processed information processed based on information decrypted by the decrypting means and with the key selected by the selecting means, using the algorithm selected by the selecting means, and a means for transmitting the cipher text generated by the encrypting means to the mobile bodies located at the prescribed position.

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-151578 ①

(P2000-151578A)

(43)公開日 平成12年5月30日(2000.5.30)

(51)Int.Cl.⁷

識別記号

F I

テマコード(参考)

H 0 4 L 9/14

H 0 4 L 9/00

6 4 1

3 E 0 2 7

G 0 7 B 15/00

G 0 7 B 15/00

L

5 J 1 0 4

5 1 0

5 1 0

5 K 0 6 7

H 0 4 Q 7/38

H 0 4 B 7/26

1 0 9 R

審査請求 未請求 請求項の数5 O L (全 16 頁)

(21)出願番号

特願平10-318605

(22)出願日

平成10年11月10日(1998.11.10)

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72)発明者 森吉 国治

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72)発明者 時田 俊雄

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74)代理人 100102439

弁理士 宮田 金雄 (外2名)

Fターム(参考) 3E027 EA01 EC07 EC10

5J104 AA34 DA03 NA40 PA01 PA11

5K067 AA30 AA34 AA35 EE02 HH36

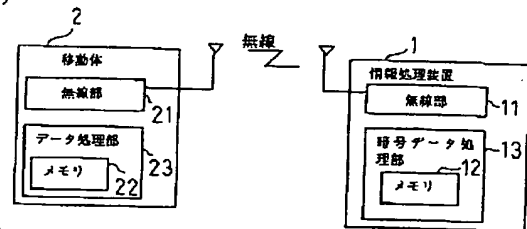
(54)【発明の名称】 暗号通信装置

(57)【要約】

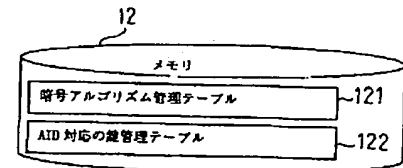
【課題】 従来の移動体と情報処理装置との間での暗号通信では、移動体において暗号化・復号化のための鍵、および暗号アルゴリズムを具備している。また、移動体、及び情報処理装置との間での通信において、使用される暗号化・復号化の鍵、および暗号アルゴリズムは各々固定されていたため、万一鍵情報が漏洩した場合は、暗号情報の盗聴やデータの改ざんの被害が拡大する危険があり、セキュリティの面から課題があった。また、移動体における暗号処理に絡むアプリケーションの種類は1種類に限定されていた。

【解決手段】 暗号アルゴリズム識別子(AID)と、AIDに対応した暗号鍵/復号鍵の鍵識別子(KID)複数個を移動体が具備し、複数の暗号アルゴリズムと、各々の暗号アルゴリズムに対応した暗号アルゴリズム識別子(AID)と、各々の暗号アルゴリズムに対応した複数の暗号鍵/復号鍵と、各々の暗号鍵/復号鍵に対応した鍵識別子(KID)とを情報処理装置が具備する。

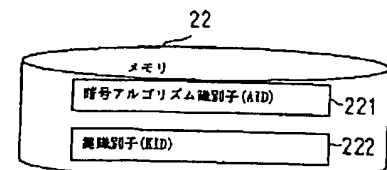
(a)



(b)



(c)



【特許請求の範囲】

【請求項1】 情報処理装置と、この情報処理装置と双方向通信を行う複数の移動体とで構成される暗号通信装置において、

上記移動体は、上記情報処理装置から送信される暗号文を受信する手段と、固有の暗号アルゴリズム識別子と鍵識別子とを格納するとともに、上記受信された暗号文を格納する第1の記憶手段と、上記情報処理装置との位置が所定位置に到達したときに、上記第1の記憶手段に格納された暗号アルゴリズム識別子と鍵識別子と暗号文とともに上記情報処理装置へ向けて送信する手段とを具備し、

上記情報処理装置は、上記所定位置に有る移動体から送信された暗号文、暗号アルゴリズム識別子、及び鍵識別子を受信する手段と、上記移動体が個々に有する暗号アルゴリズム識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する鍵識別子にそれぞれ対応した異なる複数の鍵を格納する第2の記憶手段と、上記第2の記憶手段に格納された複数のアルゴリズムから受信された暗号アルゴリズム識別子に対応するアルゴリズムを選択する手段、及び上記第2の記憶手段に記憶された複数の鍵から受信された暗号アルゴリズム識別子に対応する鍵を選択する手段を有する選択手段と、上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで受信された暗号文を復号化する復号化手段と、上記復号化手段で復号化された情報に基づいて処理された処理情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、上記暗号化手段で生成された暗号文を上記所定位置に有る移動体へ向けて送信する手段とを具備したことを特徴とする暗号通信装置。

【請求項2】 情報処理装置と、この情報処理装置と双方向通信を行う複数の移動体とで構成される暗号通信装置において、

上記移動体は、上記情報処理装置から送信される暗号文を受信する手段と、固有の複数の異なる暗号アルゴリズム識別子と複数の異なる鍵識別子とを格納するとともに、上記受信された暗号文を格納する第1の記憶手段と、上記情報処理装置との位置が所定位置に到達したときに、上記第1の記憶手段に記憶された暗号アルゴリズム識別子と鍵識別子と上記第1の記憶手段に格納された暗号文とともに上記情報処理装置へ向けて送信する手段とを具備し、

上記情報処理装置は、上記所定位置に有る移動体から送信された暗号文、暗号アルゴリズム識別子、及び鍵識別子を受信する手段と、上記移動体が個々に有する暗号アルゴリズム識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する鍵識別子にそれぞれ対応した異なる複数の鍵を格納する第2の記憶手

段と、上記第2の記憶手段に記憶された複数のアルゴリズムから受信された暗号アルゴリズム識別子に対応するアルゴリズムを選択する手段、及び上記記憶手段に記憶された複数の鍵から受信された暗号アルゴリズム識別子に対応する鍵を選択する手段を有する選択手段と、上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで上記受信された暗号文を復号化する復号化手段と、上記復号化手段で復号化された情報に基づいて処理された処理情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、上記暗号化手段で生成された暗号文を上記所定位置に有る移動体へ向けて送信する手段とを具備したことを特徴とする暗号通信装置。

【請求項3】 上記情報処理装置の上記選択手段は、上記受信した暗号識別子または鍵識別子を変更する手段と、上記第2の記憶手段に記憶された複数のアルゴリズムから上記受信した暗号アルゴリズム識別子あるいは上記変更された暗号アルゴリズム識別子のいずれか一方に対応するアルゴリズムを選択する手段、及び上記記憶手段に記憶された複数の鍵から上記受信した鍵識別子あるいは上記変更された鍵識別子のいずれか一方に対応する鍵とを選択する手段を備え、上記情報処理装置の送信手段は、上記暗号化手段で生成された暗号文とともに上記受信された暗号アルゴリズム識別子、及び鍵識別子を上記所定位置に有る移動体へ向けて送信する手段を備えたことを特徴とする請求項1もしくは2記載の暗号通信装置。

【請求項4】 情報処理装置と、この情報処理装置と双方向通信を行う複数の移動体とで構成される暗号通信装置において、

上記移動体は、上記情報処理装置から送信される暗号文を受信する手段と、固有の移動体識別子とを格納するとともに、上記受信された暗号文を格納する第1の記憶手段と、上記情報処理装置との位置が所定位置に到達したときに、上記第1の記憶手段に格納された移動体識別子と暗号文とともに上記情報処理装置へ向けて送信する手段とを具備し、

上記情報処理装置は、上記所定位置に有る移動体から送信された暗号文、及び移動体識別子を受信する手段と、上記移動体が個々に有する移動体識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する移動体識別子にそれぞれ対応した異なる複数の鍵を格納する第2の記憶手段と、上記第2の記憶手段に記憶された複数のアルゴリズムから受信された移動体識別子に対応するアルゴリズムを選択する手段、及び上記第2の記憶手段に記憶された複数の鍵から受信された移動体識別子に対応する鍵を選択する手段を有する選択手段と、上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで上記移動体からの暗号

文を復号化する復号化手段と、上記復号化手段で復号化された情報に基づいて処理された情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、上記暗号化手段で生成された暗号文を上記所定位置に有る移動体へ向けて送信する手段とを具備したことを特徴とする暗号通信装置。

【請求項5】 上記暗号化手段は、上記復号化された情報に基づいて利用料金を計算し、上記復号化された情報の有する所持金とこの計算された利用料金との差から新たな所持金を計算し、この計算された所持金と当該情報処理装置に固有の情報とから上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する手段を備えたことを特徴とする請求項1から4記載の暗号通信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、無線通信機能を有する移動体と情報処理装置との間での移動体通信システムにおいて通信情報を秘匿する暗号通信装置に関するものである。

【0002】

【従来の技術】近年、携帯電話、自動車電話、テレターミナルシステム等の移動体通信システムにおいて、通信の秘匿のために暗号が利用される。一般的な移動体通信システムにおける暗号通信方式の運用の一例として特開平1-307341号公報に開示されるようなテレターミナルシステムを以下に示す。図8にそのテレターミナルシステムの構成例を示し、図8(a)はシステム構成を示し、図8(b)は移動体のデータ処理部が有するメモリの構成を示し、図8(c)は情報処理装置のデータ処理部が有するメモリの構成を示すものである。図8

(a)において、無線部31、及びデータ処理部33を有する携帯端末のような移動体3と、無線部41、及びデータ処理部43を有する地上の情報処理装置(固定設備)4とが無線接続されており、この間のデータ通信においてはデータの盗聴・漏洩を防ぐために暗号通信処理が行われる。また、図8(b)において移動体3のデータ処理部33は、暗号アルゴリズム321、及び原始鍵322と原始鍵を元に新たに生成するDES暗号鍵323が保持されるメモリ32を具備している。また、図8(c)において、情報処理装置4のデータ処理部43は、暗号アルゴリズム421、原始鍵422、及び原始鍵を元に新たに生成されるDES暗号鍵423が保持されるメモリ42を具備している。図9は、テレターミナルシステムの暗号通信方式の例を示すフローチャートである。

【0003】なお、図9において情報処理装置4の1台に対して、情報処理装置4と通信を行う移動体3は3a以外にも複数(移動体3b・・・移動体3n)存在す

る。

【0004】図8、および図9に示した従来の暗号通信方式実施例の動作を以下に説明する。

【0005】まず、移動体3a、および情報処理装置4の各々において、メモリ32に記憶された原始鍵 α またはメモリ42に記憶された原始鍵 β による公開鍵Xまたは公開鍵Yが生成され、この公開鍵を互いに送信することによって公開鍵を共有する(処理S101、処理S103)。つぎに、移動体3aにおいては、原始鍵 α と情報処理装置から受信した公開鍵YによるDES暗号鍵Zの生成を行い(処理S104)、一方情報処理装置4では、原始鍵 β と移動体3aから受信した公開鍵XによるDES暗号鍵Zの生成が行われる(処理S102)。なお、このとき移動体3aと情報処理装置4は共通のDES暗号鍵Zを所有し、それぞれメモリ32およびメモリ42に保持することになる。

【0006】つぎに、移動体3aにおいて、DES暗号鍵Zによる送信文の暗号化を行って暗号文を生成し(処理S105)、この暗号文を情報処理装置4へ送信する(処理S106)。

【0007】つぎに、情報処理装置4において、移動体3aからの暗号文が受信される(処理S107)。この暗号文がDES暗号鍵Zで復号化され、平文が生成される(処理S108)。生成された平文に対して情報処理装置4において内部処理が行われ、この処理結果に基づき移動体への送信文が生成される。この生成された送信文(平文)が移動体3aへ送信するためにDES暗号鍵Zで暗号化されて暗号文が生成され、この暗号文が移動体3aへ送信される(処理S109)。つぎに、移動体3aにおいて情報処理装置4からの暗号文を受信し、DES暗号鍵Zによる暗号文の復号化が行われ、平文化することによって移動体での送信文の内部処理が行われる(処理S110)。

【0008】以上の動作により、移動体3aと情報処理装置4との間で暗号通信が行われる。

【0009】また、移動体3bから3nと情報処理装置4との間においても、上記の手順と同様にして、暗号通信が行われる。

【0010】一方、上記のテレターミナルシステム等のような移動体通信システムとは別に、近年、有料道路を利用する車両に搭載された車載機(移動体)と料金所との間で双方向通信を行い、その車載機から通行料を課金する料金収受システムのような移動体通信システムが提案されている。

【0011】図10は、この種の料金収受システムの使用形態の一例を示したものである。図において、車載機5を搭載した車両6が情報処理装置7に接続された料金所8の所定位置に接近すると、例えば料金所8に設けられた撮像機9が車両6のナンバープレートを読み取る、あるいは料金所7に設けられた無線アンテナ10が移動

体から発信される固有の識別信号を受信することにより、車両6と情報処理装置7との間で互いに相手の正当性を認証する相互認証処理が行われる。相互認証処理で認証された車両6は、内部のメモリーに保持された契約情報（顧客番号、車両の種別等）と利用情報（有料道路の入口料金所の情報、利用時間等）を車載機5の無線アンテナ10から送信する。情報処理装置7は、料金所8に設けられた無線アンテナ10を介してこの車両6からの送信データを受信後、その受信された契約情報や利用情報に基づいて利用料金（通行料金）を計算し、無線アンテナ10を介して車載機5にその利用料金を送信する。車載機5は、情報処理装置7からの利用料金を受信すると、内部のメモリーに記憶された所持金からこの利用料金を減算して所持金を更新し、内部のメモリーに格納する。

【0012】この種の料金収受システムのような移動体通信システムにおいても、無線通信される利用情報や利用料金の盗聴、漏洩を防ぐために、データの秘匿が不可欠となる。このため、上述のテレターミナルシステム等の移動体通信システムと同様の図8、9に示すような暗号通信方式を利用したシステムが提案されている。

【0013】

【発明が解決しようとする課題】従来の移動体と情報処理装置との間での暗号通信では、以上のように情報処理装置だけでなく、移動体においても暗号化・復号化のための鍵（暗号鍵、復号鍵）、および暗号アルゴリズムを具備している。また、移動体、および情報処理装置との間での通信において、使用される暗号化・復号化のための鍵（暗号鍵、復号鍵）、および暗号アルゴリズムは固定されていて、公開鍵と共通鍵で各々1種類である。このため、不特定多数の所有者が存在する移動体において、万一移動体での鍵管理が不徹底のために鍵情報が漏洩した場合は、鍵、および暗号アルゴリズムは1種類で固定されているので、暗号情報の盗聴やデータの改ざんの被害が拡大する危険があり、セキュリティの面から課題があった。また、移動体における暗号処理に絡むアプリケーションの種類は1種類に限定されていた。

【0014】この発明は、上述のような課題を解決するためになされたもので、複数の暗号アルゴリズム、および当該暗号アルゴリズムに対応した複数の暗号鍵／復号鍵をシステムにて利用可能とすることにより、前記移動体が各々の暗号アルゴリズム処理、および当該暗号アルゴリズムに対応した暗号鍵／復号鍵の処理によるアプリケーション機能を実現し、かつ前記移動体が有する暗号文に対するセキュリティを確保して当該移動体と情報処理装置において暗号通信処理が可能な暗号通信装置を提供することを目的とするものである。

【0015】

【課題を解決するための手段】第1の発明による暗号通信装置は、情報処理装置と、この情報処理装置と双方向

通信を行う複数の移動体とで構成される暗号通信装置において、上記移動体は、上記情報処理装置から送信される暗号文を受信する手段と、固有の暗号アルゴリズム識別子と鍵識別子とを格納するとともに、上記受信された暗号文を格納する第1の記憶手段と、上記情報処理装置との位置が所定位置に到達したときに、上記第1の記憶手段に格納された暗号アルゴリズム識別子と鍵識別子と暗号文とともに上記情報処理装置へ向けて送信する手段とを具備し、上記情報処理装置は、上記所定位置に有る移動体から送信された暗号文、暗号アルゴリズム識別子、及び鍵識別子を受信する手段と、上記移動体が個々に有する暗号アルゴリズム識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する鍵識別子にそれぞれ対応した異なる複数の鍵を格納する第2の記憶手段と、上記第2の記憶手段に格納された複数のアルゴリズムから受信された暗号アルゴリズム識別子に対応する鍵を選択する手段、及び上記第2の記憶手段に記憶された複数の鍵から受信された暗号アルゴリズム識別子に対応するアルゴリズムを選択する手段を有する選択手段と、上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで受信された暗号文を復号化する復号化手段と、上記復号化手段で復号化された情報に基づいて処理された処理情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、上記暗号化手段で生成された暗号文を上記所定位置に有る移動体へ向けて送信する手段とを具備したものである。

【0016】第2の発明による暗号通信装置は、情報処理装置と、この情報処理装置と双方向通信を行う複数の移動体とで構成される暗号通信装置において、上記移動体は、上記情報処理装置から送信される暗号文を受信する手段と、固有の複数の異なる暗号アルゴリズム識別子と複数の異なる鍵識別子とを格納するとともに、上記受信された暗号文を格納する第1の記憶手段と、上記情報処理装置との位置が所定位置に到達したときに、上記第1の記憶手段に格納された暗号アルゴリズム識別子と鍵識別子と上記第1の記憶手段に格納された暗号文とともに上記情報処理装置へ向けて送信する手段とを具備し、上記情報処理装置は、上記所定位置に有る移動体から送信された暗号文、暗号アルゴリズム識別子、及び鍵識別子を受信する手段と、上記移動体が個々に有する暗号アルゴリズム識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する鍵識別子にそれぞれ対応した異なる複数の鍵を格納する第2の記憶手段と、上記第2の記憶手段に記憶された複数のアルゴリズムから受信された暗号アルゴリズム識別子に対応するアルゴリズムを選択する手段、及び上記記憶手段に記憶された複数の鍵から受信された暗号アルゴリズム識別子に対応する鍵を選択する手段を有する選択手段と、上記

選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで上記受信された暗号文を復号化する復号化手段と、上記復号化手段で復号化された情報に基づいて処理された処理情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、上記暗号化手段で生成された暗号文を上記所定位置に有る移動体へ向けて送信する送信手段とを具備したものである。

【0017】第3の発明による暗号通信装置は、第1もしくは第2の発明において、上記情報処理装置の上記選択手段は、上記受信した暗号アルゴリズム識別子または鍵識別子を変更する手段と、上記第2の記憶手段に記憶された複数のアルゴリズムから上記受信した暗号アルゴリズム識別子あるいは上記変更された暗号アルゴリズム識別子のいずれか一方に対応するアルゴリズムを選択する手段、及び上記記憶手段に記憶された複数の鍵から上記受信した鍵識別子あるいは上記変更された鍵識別子のいずれか一方に対応する鍵とを選択する手段を備え、上記情報処理装置の送信手段は、上記暗号化手段で生成された暗号文とともに上記受信された暗号アルゴリズム識別子、及び鍵識別子を上記所定位置に有る移動体へ向けて送信する手段を備えたものである。

【0018】第4の発明による暗号通信装置は、情報処理装置と、この情報処理装置と双方向通信を行う複数の移動体とで構成される暗号通信装置において、上記移動体は、上記情報処理装置から送信される暗号文を受信する手段と、固有の移動体識別子とを格納するとともに、上記受信された暗号文を格納する第1の記憶手段と、上記情報処理装置との位置が所定位置に到達したときに、上記第1の記憶手段に格納された移動体識別子と暗号文とともに上記情報処理装置へ向けて送信する手段とを具備し、上記情報処理装置は、上記所定位置に有る移動体から送信された暗号文、及び移動体識別子を受信する手段と、上記移動体が個々に有する移動体識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する移動体識別子にそれぞれ対応した異なる複数の鍵を格納する第2の記憶手段と、上記第2の記憶手段に記憶された複数のアルゴリズムから受信された移動体識別子に対応するアルゴリズムを選択する手段、及び上記第2の記憶手段に記憶された複数の鍵から受信された移動体識別子に対応する鍵を選択する手段を有する選択手段と、上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで上記移動体からの暗号文を復号化する復号化手段と、上記復号化手段で復号化された情報に基づいて処理された情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、上記暗号化手段で生成された暗号文を上記所定位置に有る移動体へ向けて送信する手段とを具備したものである。

【0019】第5の発明による暗号通信装置は、第1の発明から第4の発明において、上記暗号化手段は、上記復号化された情報に基づいて利用料金を計算し、上記復号化された情報の有する所持金とこの計算された利用料金との差から新たな所持金を計算し、この計算された所持金と当該情報処理装置に固有の情報とから上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する手段を備えたものである。

【0020】

【発明の実施の形態】実施の形態1．従来の移動体通信システムでは、移動体と情報処理装置の双方で同じ暗号アルゴリズム、および暗号化・復号化に用いる共通な鍵を備えて、通信情報を秘匿する暗号通信が行われていた。特に、図10に示すような料金收受システムでは、移動体（車載機5）が料金所の所定位置に到達したとき、移動体と情報処理装置との間で相互認証処理が行われ、認証された移動体が料金所に設けられた情報処理装置へ向けて契約情報および利用情報を暗号化された暗号文として送信し、情報処理装置がその暗号文を復号化し、復号化された平文に基づいて移動体の利用料金が計算される。情報処理装置は、その計算結果を暗号化して移動体へ送信し、移動体の課金が行われる。このとき、従来の料金收受システムでは、移動体は暗号化された利用料金を受信後に、受信された利用料金を復号化し、内部メモリに格納された所持金から復号化された利用料金を差し引いた残金を新たな所持金として計算し、その計算結果を内部メモリに格納していた。しかし、このような移動体通信においては、移動体が契約情報および利用情報に加えて残金を情報処理装置に送信後、情報処理装置が、移動体から送信された契約情報および利用情報に基づいて利用料金を計算し、また移動体から送信された所持金からその利用料金を差し引いて新たな所持金を計算し、その計算結果を移動体に送信するような利用形態も想定される。この利用形態においては、移動体と情報処理装置間で通信される暗号文の暗号化や復号化を情報処理装置が行い、情報処理装置から送信される暗号文を移動体の内部メモリに格納することによって、移動体では暗号文の生成や復号化を行わず、すなわち移動体に暗号アルゴリズムを持たせずに通信情報を秘匿することができる。この発明の実施の形態1は、このような運用に基づいて行われるもので、通信される暗号文の暗号化および復号化を情報処理装置のみで行い、移動体は、暗号文とともにその暗号文を暗号化するための暗号アルゴリズムと鍵を識別する識別子を情報処理装置へ送信し、情報処理装置は、その識別子に対応する暗号アルゴリズムと鍵によって暗号化された暗号文を移動体へ送信する暗号通信装置を提供するものである。以下、この発明による暗号通信装置の実施の形態を図に基づいて説明する。

【0021】図1は、実施の形態1を示す構成図で、図1(a)は移動体通信システムの構成、図1(b)は図1(a)の情報処理装置1のメモリ12、図1(c)は図1(a)の移動体2のメモリ22を示すものである。同図(a)において、1は図10に示された料金所8に設けられた情報処理装置、2は図10に示された車両6に設けられた車載機5のように情報処理装置1と通信を行う移動体、11は情報処理装置1の無線部、21は移動体2の無線部、12は情報処理装置1の暗号データ処理部13のメモリ、22は移動体2のデータ処理部23のメモリである。メモリ22は移動体2が情報処理装置1と送受信を行うための暗号文を格納するために、またメモリ12は情報処理装置1が移動体2と送受信を行うための暗号文を格納したり、暗号化・復号化の処理や内部処理(例えば料金計算処理等)を行うために使用する。尚、情報処理装置1の1台が処理対象とする移動体2は複数台存在する。同図(b)は情報処理装置1のメモリ12を示すもので、暗号文の格納領域の他に、暗号アルゴリズム管理テーブル121、および暗号アルゴリズム識別子(以下AIDと称する)対応の鍵管理テーブル122を具備している。同図(c)は移動体2のメモリ22を示すもので、暗号文や内部処理のための格納領域の他に、221および222の領域にAID、および鍵識別子(以下KIDと称する)が格納されている。AID、KIDは情報処理装置側で管理する識別子であり、個々の識別子が区別できるものであれば、例えば文字列と数字の組み合わせ(AID1、AID2、・・・AIDn)(KID1、KID2、・・・KIDn)やビットアサイン(数)による識別でよい。

【0022】図2は、図1(b)における情報処理装置1がメモリ12に保持する暗号アルゴリズム管理テーブル121の詳細図である。同図において、121はシステムで定めている暗号アルゴリズムの識別子AID(1)からAID(K)までの管理テーブル、AID(1)からAID(K)に対応する暗号アルゴリズム1211のインデックス(メモリアドレス)、およびAID(K)対応の鍵管理テーブル122のインデックス(メモリアドレス)を含む。

【0023】図3は、図1における情報処理装置が保持するAID(K)対応の鍵管理テーブル122であり、暗号鍵/復号鍵の鍵識別子KID、およびKID対応の鍵(暗号鍵/復号鍵)を示すもので、一つのAIDに対して、KIDとKID対応の鍵がn個設定される。同図において、1221は一つのAIDに対するn番目の鍵識別子KID(n)であり、1222はKID(n)対応の鍵を指す。

【0024】次に動作について説明する。本発明では、移動体では暗号アルゴリズムを具備しておらず、データが暗号化された状態のままで保存されることが前提となる。図4は、実施の形態1の処理手順を示すフローチャ

ートである。図4における処理手順について述べる。まず、移動体2が情報処理装置7の設けられた料金所の所定位置に接近すると、相互認証の結果認証された移動体2にて情報処理装置1へ送信する暗号文とその暗号文に対応するAID、KIDを移動体のメモリ22から得る(処理S1)。この時、例えば暗号文として契約情報(顧客番号、移動体の種別等)や利用情報(有料道路の場合は前回通過した料金所にて送信された入口料金所の情報を示す入口情報、有料設備の場合は利用開始時間等)と移動体2の電子的に有する貨幣と等価な所持金の情報を得る。つぎに、このAID、KID、および暗号文を情報処理装置1へ送信する(処理S2)。情報処理装置1では移動体2からAID、KID、および暗号文を受信後(処理S3)、メモリ12のアルゴリズム管理テーブル121より該当AIDの暗号アルゴリズムを選択する(処理S4)、AID対応の鍵管理テーブル、およびKIDより暗号鍵/復号鍵を選択する(処理S5)。つぎに、選択された復号鍵をキーにして移動体2からの暗号文を選択された暗号アルゴリズムで復号して内部処理を行う(処理S6)。内部処理として、例えば、有料道路・有料設備の利用料金計算処理等を行う。有料道路利用の出口料金所の場合は、移動体2より受け取った顧客番号、移動体の種別(車両の種別)、入口情報と情報処理装置1の所在する出口料金所の情報に基づいて、情報処理装置が移動体2から受け取った所持金から利用料金(通行料金)を差し引いた残金を、新たな所持金として計算し、入口情報を初期値にする。また、入口料金所の場合は、入口情報のみ更新し、入口料金所の識別情報を付加する。この内部処理の結果得られる所持金と入口情報と契約情報から、暗号鍵をキーにして移動体への送信暗号文(応答暗号文)を生成し、移動体2へ送信する(処理S7)。移動体2では、情報処理装置1からの応答暗号文を受信(処理S8)して、受信暗号文のメモリ22への格納等の内部処理を行う(処理S9)。この結果、移動体2では、新たな所持金を暗号化された状態でメモリ22へ格納することになる。

【0025】以上のように、この実施の形態1の複数暗号処理方式によれば、AIDとAIDに対応したKIDを移動体2が具備することで、移動体2では暗号化・復号化を行わず、情報処理装置1に暗号化・復号化の処理を任せることができる。尚、AID、KID、契約情報、利用情報、および所持金は移動体がシステム加入時(契約時)、システムによって移動体2に固定情報として組み込まれる。また、この所持金は、プリペイドカードのように貨幣に等しいものの以外の、例えば、クレジットカードのように電子決済されて移動体利用者の銀行口座から引き落とされるものでもよい。この場合、情報処理装置2が所持金の情報を銀行との間で送受信する。また、本方式では移動体2の内部には暗号アルゴリズムや暗号鍵・復号鍵を保有していないので、情報処理装置1

のAID対応の鍵管理テーブル情報を盗まれない限り、移動体2の暗号化情報に対するセキュリティ確保に貢献できる。尚、上述の例は移動体(車両)が有料道路・設備を利用する料金収受システムについて示したが、移動体としては無線部、CPU、メモリを有するICカードであっても本発明は適用できる。また、移動体2のメモリ22に記憶される暗号文は、所持金の代わりに利用料金であってもよい。この場合、情報処理装置1は、移動体2の利用者の銀行口座から、この利用料金を差し引くような電子決済を行う。

【0026】実施の形態2。図5は、実施の形態2を示す構成図で、図5(a)は移動体通信システムの構成、図5(b)は図5(a)の移動体2のメモリ22、図5(c)は図5(b)のAID・KID対応テーブル223を示すものである。図5において、1は情報処理装置、2は移動体、223は移動体2のメモリ22が具備するAID・KID対応テーブルである。

【0027】次に動作について説明する。移動体2は、AID・KID対応テーブル223を具備しており、このAID・KID対応テーブル223により、システムで決められた複数の暗号アルゴリズムに対応する暗号アルゴリズム識別子(AID)、および各々の暗号アルゴリズムに対応する複数の暗号鍵/復号鍵の鍵識別子(KID)を保持することになる。この仕組みにより、移動体2と情報処理装置1とにおいて、複数の暗号アルゴリズム、および各々の暗号アルゴリズムに対応する複数の暗号鍵/復号鍵による暗号情報の送信・受信を行えるようになる。

【0028】以上のように、移動体2が具備するAIDとKIDの組み合わせが複数ある場合でも、移動体2が格納している各々の暗号化情報に対応するAID、KIDを暗号化情報とともに情報処理装置1に送信することで、情報処理装置1に暗号化・復号化の処理を任せることができる。

【0029】実施の形態3。図6は、実施の形態3による複数暗号処理方式を示す構成図である。同図において、情報処理装置1は、暗号アルゴリズム管理テーブル、およびAID対応の鍵管理テーブルを具備している。移動体2は、AID・KID対応テーブル223を具備し、AID・KID対応テーブル223には各AIDに対応したKIDテーブルが含まれる。

【0030】次に動作について説明する。移動体2が保持している暗号データと、その暗号データに関連するAID、およびAID・KID対応テーブル223中のKIDテーブルから選択されたKIDが、情報処理装置1へ送信される。情報処理装置1において、移動体2より受信したAID、KIDを基にして、暗号アルゴリズム管理テーブル、AID対応の鍵管理テーブルから該当する暗号アルゴリズムと鍵を検出する。次に、この鍵で移動体2より受信した暗号データの復号化を行い、平文を

得て内部処理を行い、移動体2への送信文(平文)を生成する。ここで、情報処理装置1において、移動体2への送信文(平文)を暗号化する際、暗号アルゴリズムや鍵を変更(更新、あるいは新規に設定)することができる。暗号アルゴリズムや鍵を変更した場合、AID、KIDも変更され、暗号化データとともに、移動体2へ送信される。移動体2では受信したAID、KIDを基に、AID・KID対応テーブル223、223のKIDテーブルの内容について、KIDの更新日を含めて更新処理を行う。

【0031】以上のように、移動体2が保持する暗号データに関するAIDとKIDを変更する方式を提供することができる。

【0032】実施の形態4。図7は、実施の形態4による複数暗号処理方式を示す構成図である。同図において、移動体2は移動体識別子(MID)224を具備している。情報処理装置1は、移動体識別子(MID)、および各MIDとAID、KIDとの対応を判別できるMID管理テーブル123を具備している。また、情報処理装置1は、MID管理テーブル123とリンクした暗号アルゴリズム管理テーブル121、暗号アルゴリズム管理テーブルとリンクしたAID対応の鍵管理テーブル122を具備している。AID対応の鍵管理テーブル122の構成は図3と同様である。実施の形態4による複数暗号処理方式によれば、移動体2は移動体識別子(MID)224を具備していて、このMIDのみを情報処理装置1へ送信することで、情報処理装置1において、MID管理テーブル123にて暗号アルゴリズム管理テーブル121、およびAID対応の鍵管理テーブル122がリンクされることになり、移動体2と情報処理装置1との間での複数暗号処理を可能とする。

【0033】

【発明の効果】この発明は、以上のように構成されるため、以下に示す効果を奏する。

【0034】第1、および第5の発明によれば、移動体が当該システムで決められた暗号アルゴリズムや暗号鍵/復号鍵を具備していなくても、その対応する暗号アルゴリズム識別子や鍵識別子を具備することによって、これらの移動体と情報処理装置において、復号処理が可能な方式を提供することができる。これによって、移動体が有する暗号文に対する高セキュリティを確保することができる。

【0035】また、第2の発明によれば、複数の暗号アルゴリズム、および当該暗号アルゴリズムに対応した複数の暗号鍵/復号鍵をシステムにて利用可能とすることにより、前記移動体が各々のアプリケーション処理に応じた暗号アルゴリズム処理、および当該暗号アルゴリズムに対応した暗号鍵/復号鍵を選択することが可能となり、各々の移動体のアプリケーションのセキュリティレベルに応じた暗号を選択することができる。

【0036】また、第3の発明によれば、移動体が具備する暗号アルゴリズム識別子と鍵識別子の変更を可能とする方式を提供することができ、暗号アルゴリズムや暗号鍵の変更に対して、柔軟に対応することができる。

【0037】また、第4の発明によれば、移動体が具備する移動体識別子を情報処理装置が認識することで、移動体がシステムで決められた複数の暗号アルゴリズムの何れで処理しても、かつ、移動体がシステムで決められた複数の暗号鍵／復号鍵の何れで処理しても、移動体と情報処理装置において暗号処理が可能な方式を提供することができる。

【図面の簡単な説明】

【図1】 この発明の実施の形態1を示す構成図である。

【図2】 この発明の実施の形態1を示す詳細構成図である。

【図3】 この発明の実施の形態1を示す詳細構成図である。

【図4】 この発明の実施の形態1の処理手順を示すフローチャートである。

【図5】 この発明の実施の形態2を示す構成図である。

【図6】 この発明の実施の形態3を示す構成図である。

【図7】 この発明の実施の形態4を示す構成図である。

【図8】 従来の移動体通信における暗号処理方式の構成図である。

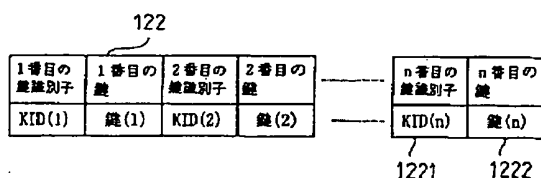
【図9】 従来の移動体通信における暗号処理方式の処理手順を示すフローチャートである。

【図10】 料金収受システムの構成例である。

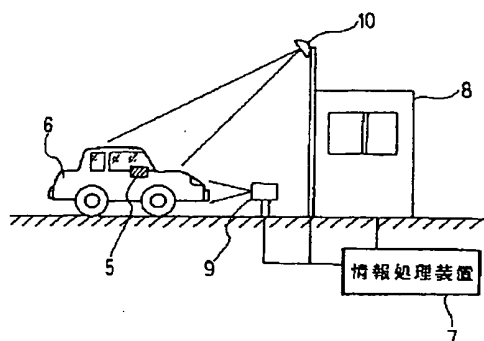
【符号の説明】

1 情報処理装置、2 移動体、3 移動体、3a 移動体、3b 移動体、4 情報処理装置、5a 移動体、5b 移動体、5n 移動体、6 情報処理装置、11 無線部、12 メモリ、21 無線部、22 メモリ、31 無線部、32 メモリ、41 無線部、42 メモリ、51 無線部、52 メモリ、53 データ処理部、61 無線部、62 メモリ、63 データ処理部、121 暗号アルゴリズム管理テーブル、122 AID対応の鍵管理テーブル、123 移動体識別子(MID)管理テーブル、221 暗号アルゴリズム識別子(AID)、222 鍵識別子(KID)、223 AID・KID対応テーブル、224 移動体識別子(MID)、321 暗号アルゴリズム、322 原始鍵、323 新しい鍵、421 暗号アルゴリズム、422 原始鍵、423 新しい鍵、521 暗号管理情報、522 暗号文、621 暗号管理情報、622 暗号文、623 平文、1211 AID(K)の暗号アルゴリズム、1221 KID(n)、1222 鍵。

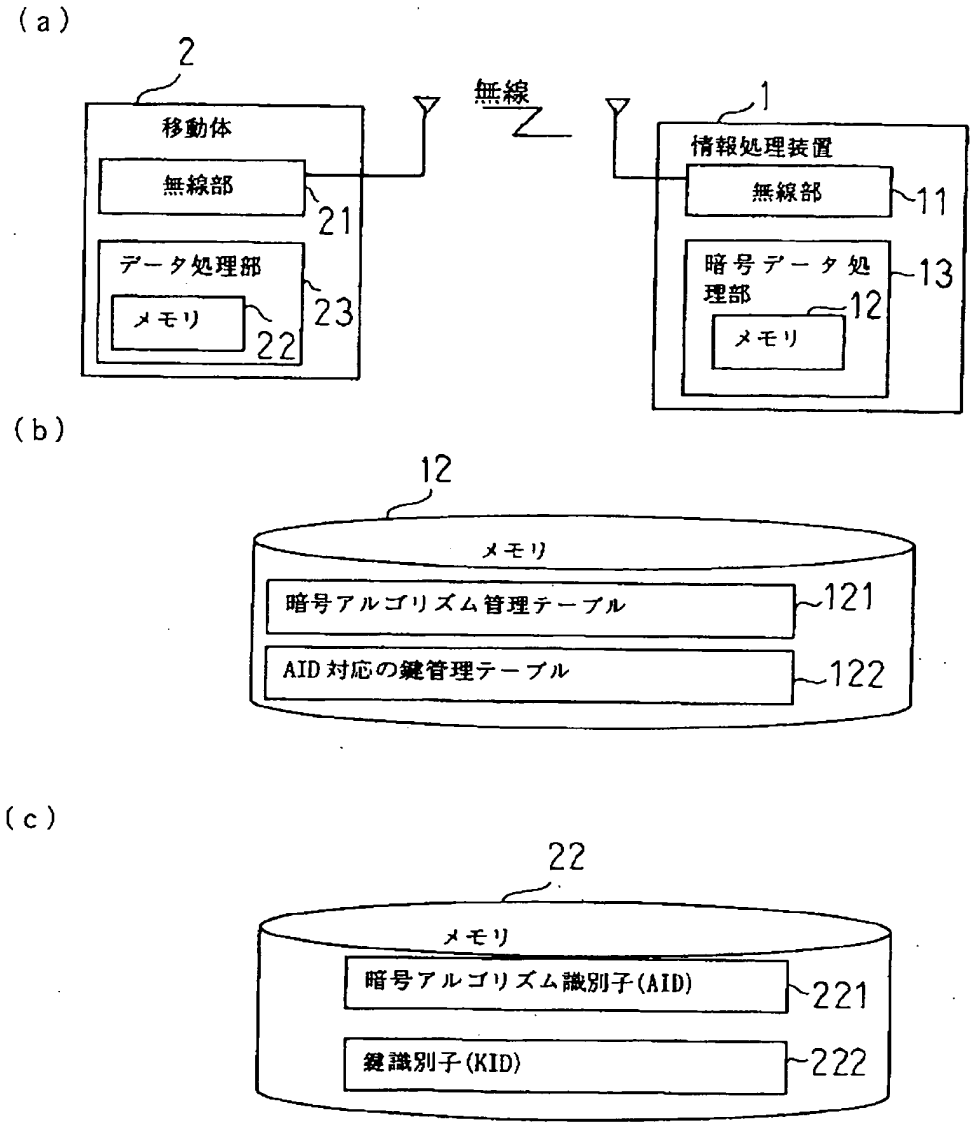
【図3】



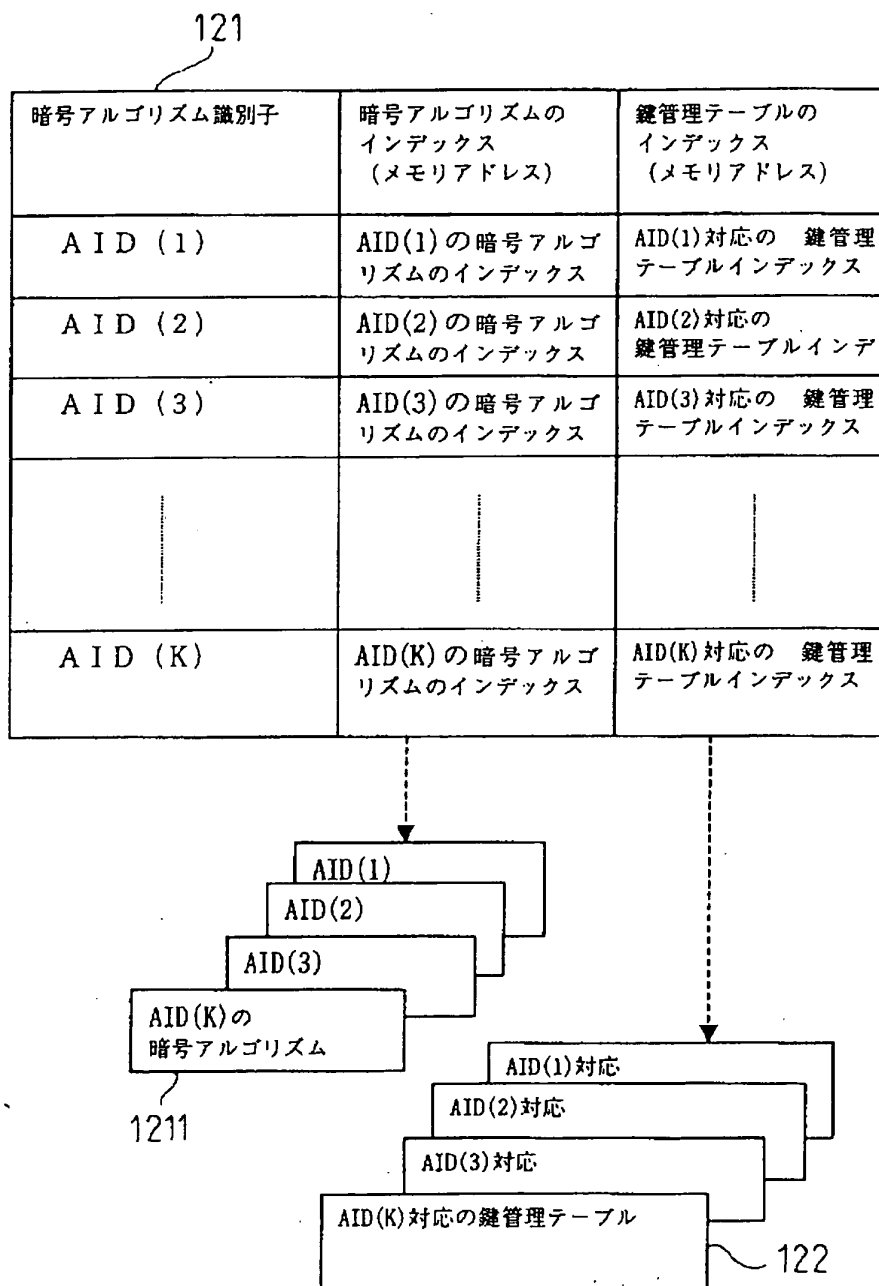
【図10】



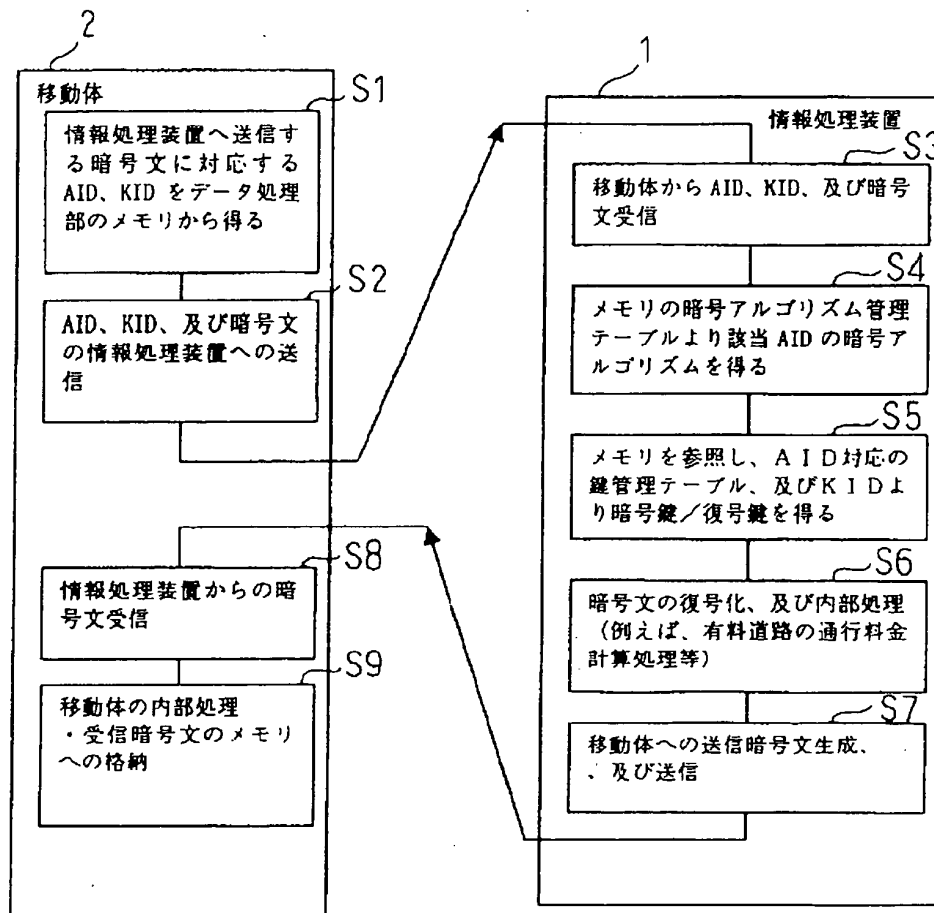
【図1】



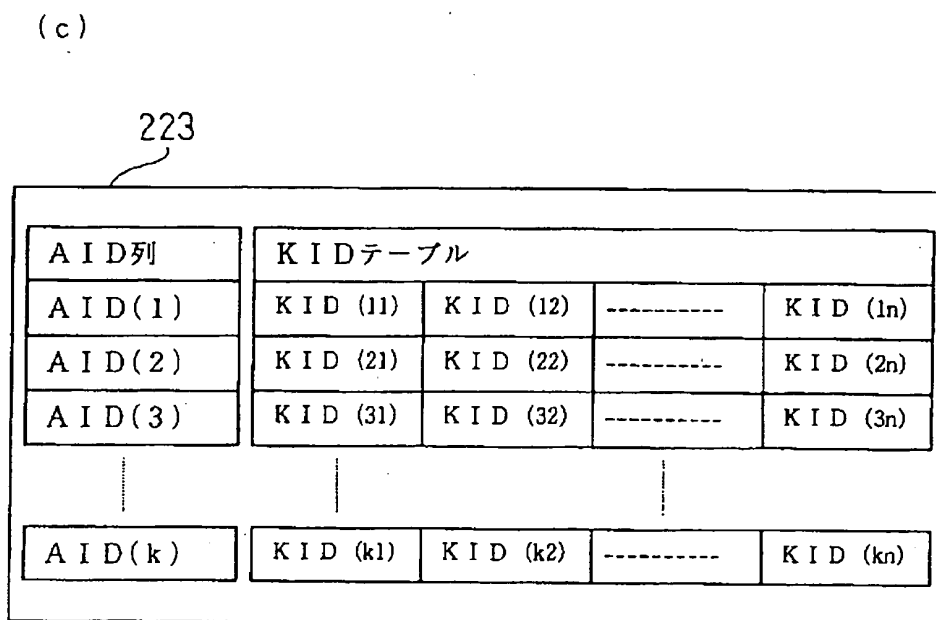
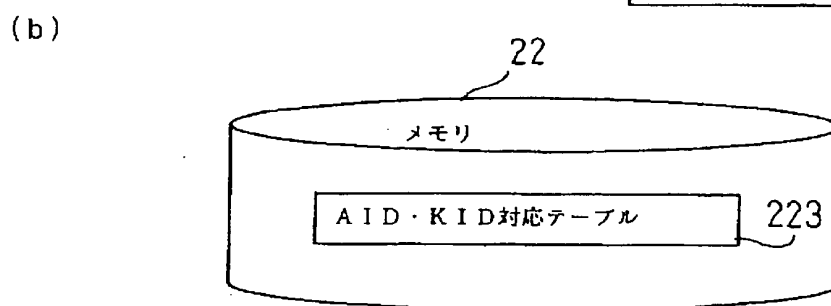
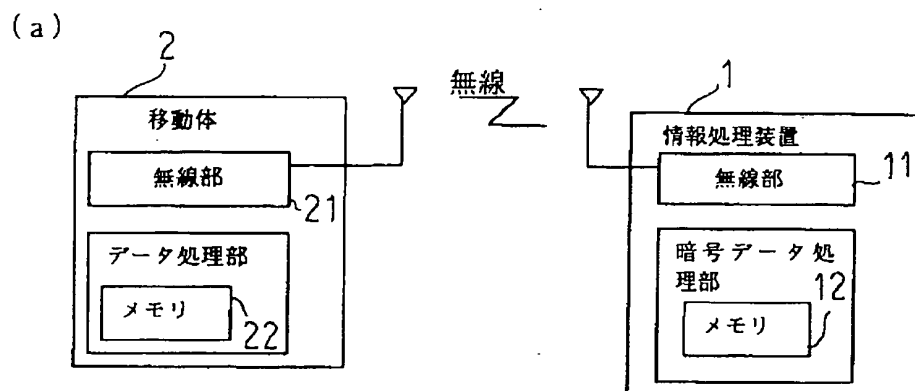
【図2】



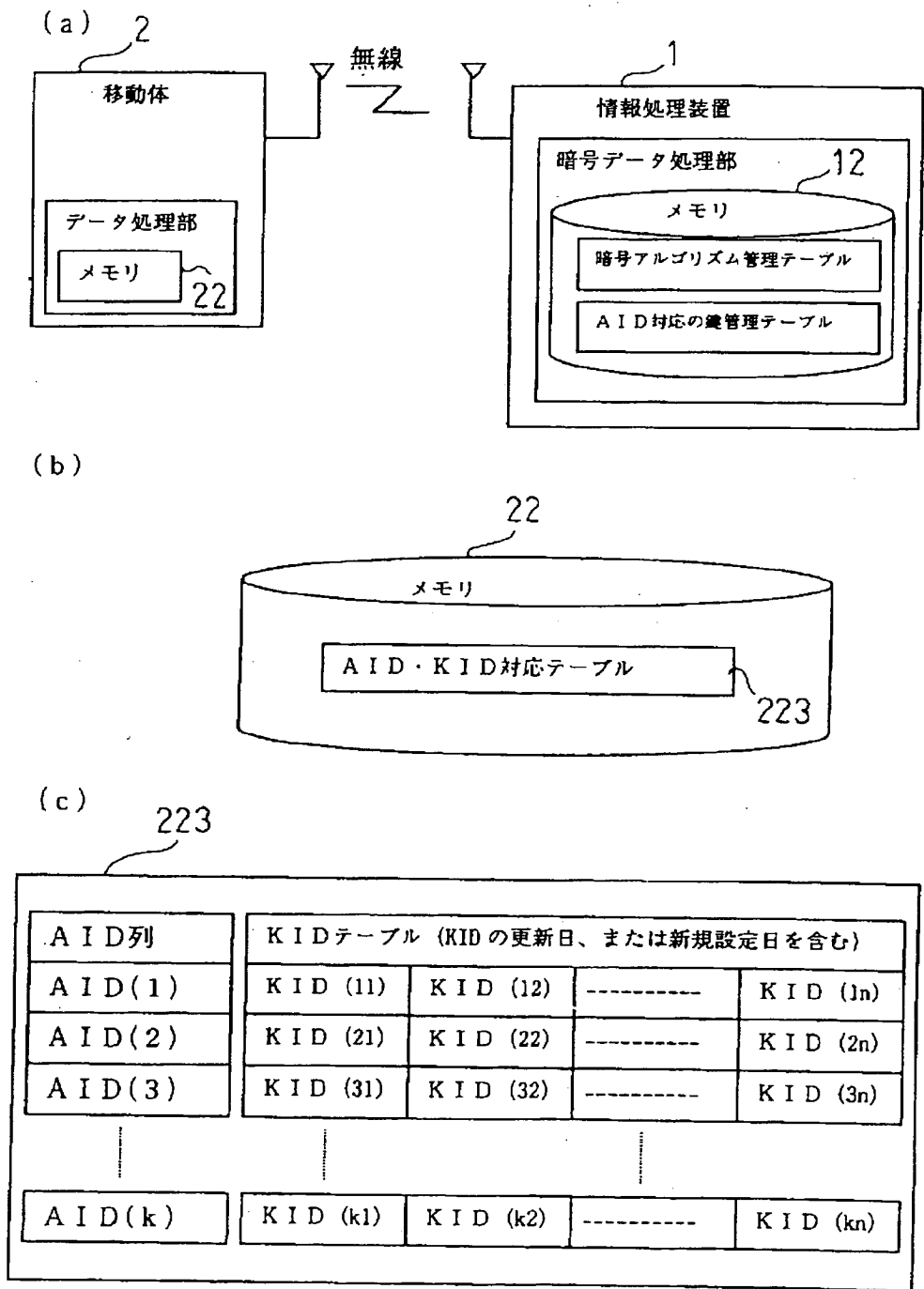
【図4】



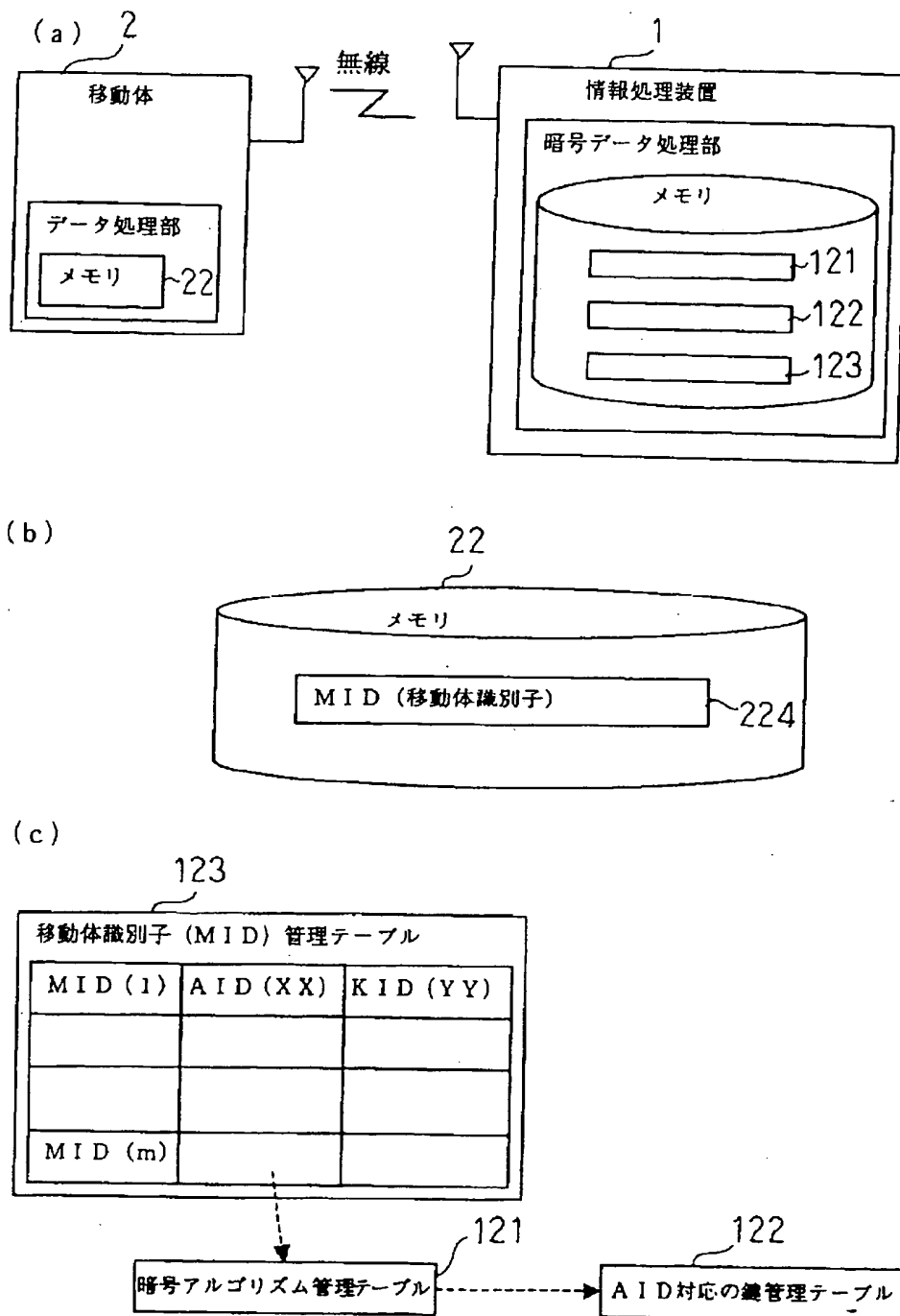
【図5】



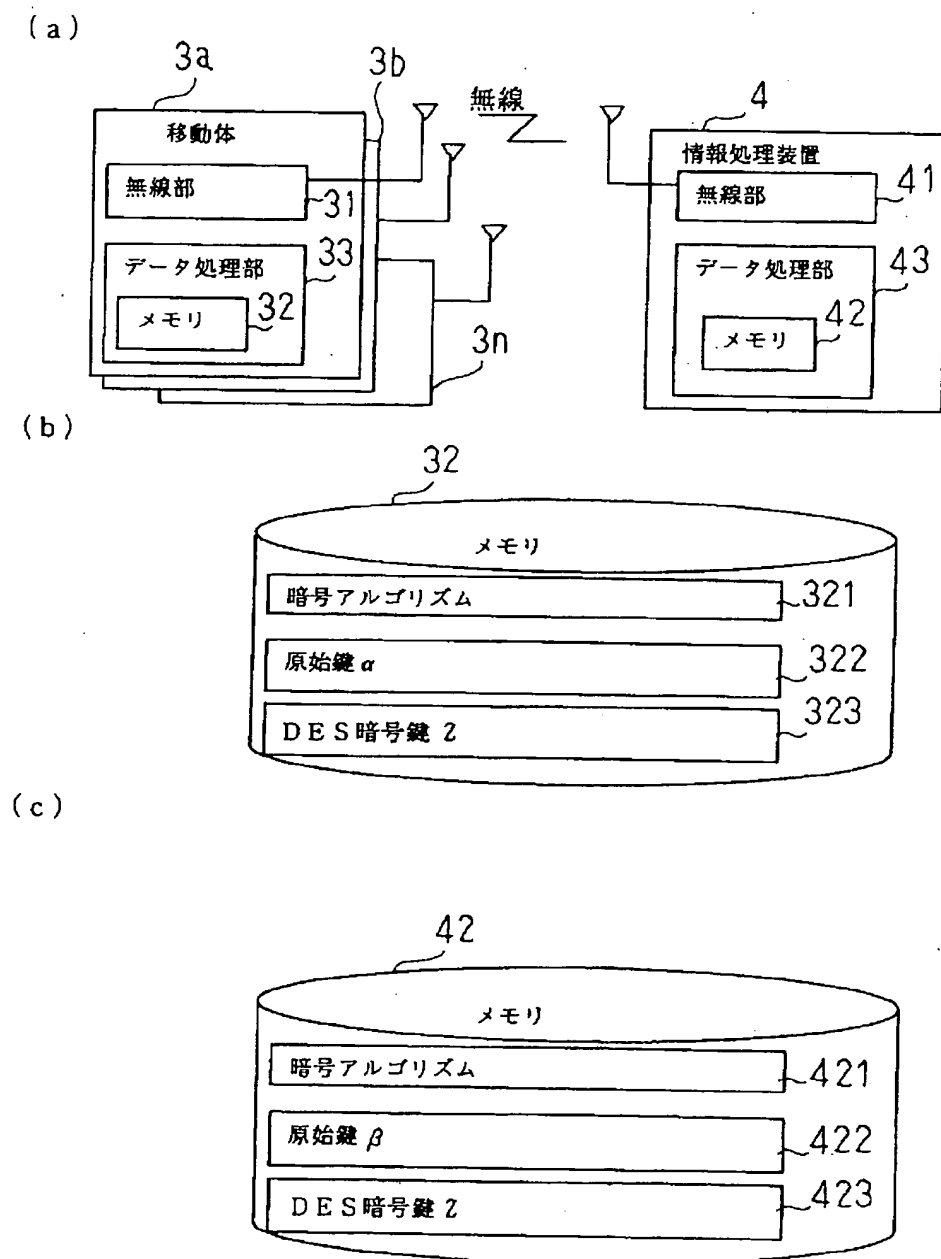
【図6】



【図7】



【図8】



【図9】

